	L #	Search Text	DBs	Time Stamp	Hits
1	L1	713/175.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/09/20 17:14	458
2	L2	enokida.in. and tomoaki.in.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/09/20 17:14	7
3	L3	ricoh.asn.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/09/20 17:14	254970

	L #	Search Text	DBs	Time Stamp	Hits
4	L4	L2 and L3	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/09/20 17:15	4
5	L5	713/156.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/09/20 17:15	911
6	L6	713/157.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/09/20 17:15	160

	L #	Search Text	DBs	Time Stamp	Hits
7	L7	713/168.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/09/20 17:15	1987
8	L8	713/169.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/09/20 17:15	437
9	L9	713/158.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/09/20 17:15	184

	L #	Search Text	DBs	Time Stamp	Hits
10	L10	713/191.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/09/20 17:15	191
11	L11	(updating) near (root key or proof key or validation or shared private key)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/09/20 17:16	1556
12	L12	L1 same (mutual authentication or certificates)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/09/20 17:17	0

	L #	Search Text	DBs	Time Stamp	Hits
13	L13	L11 same (mutual authentication or certificates)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/09/20 17:17	156
14	L14	L1 and L13	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/09/20 17:17	6
15	L15	L5 and L13	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/09/20 17:17	12

	L #	Search Text	DBs	Time Stamp	Hits
16	L16	L6 and L13	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/09/20 17:17	2
17	L17	L7 and L13	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/09/20 17:17	14
18	L18	L8 and L13	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/09/20 17:17	5

	L #	Search Text	DBs	Time Stamp	Hits
19	L19	L9 and L13	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/09/20 17:17	2
20	L20	L10 and L13	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/09/20 17:17	1
21	L21	L13 and "third party"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/09/20 17:29	53

	L #	Search Text	DBs	Time Stamp	Hits
22	L22	L21 and "digital certificate"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/09/20 17:30	15
23	L23	L22 and "server" and "client"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/09/20 17:31	11

Interference Search

	Type	L #	Search Text	DBs	Time Stamp	Hits
24	BRS	L24	digital AND certificate AND client AND server AND authentication.CLM.	US-PGPUB	2007/09/20 18:59	1649
25	BRS	L25	digital AND certificate AND client AND server AND authentication AND data AND transmission AND communication.CLM.	US-PGPUB	2007/09/20 18:59	1756
26	BRS	L26	digital AND certificate AND client AND server AND authentication AND data AND transmission AND communication AND proof AND key AND updating.CLM.	US-PGPUB	2007/09/20 19:00	56
27	BRS	L27	digital AND certificate AND client AND server AND authentication AND data AND transmission AND communication AND proof AND key AND updating AND validity AND control AND unit.CLM.	US-PGPUB	2007/09/20 19:01	34
28	BRS	L28	digital AND certificate AND client AND server AND authentication AND data AND transmission AND communication AND proof AND key AND updating AND validity AND control AND unit AND SSL AND TLS AND protocol.CLM.	US-PGPUB	2007/09/20 19:02	16
29	BRS	L29	digital AND certificate AND client AND server AND authentication AND data AND transmission AND communication AND proof AND key AND updating AND validity AND control AND unit AND SSL AND TLS AND protocol AND mutual AND authentication.CLM.	US-PGPUB	2007/09/20 19:02	5

	Comments
24	
25	
26	
27	
28	
29	

	Type	L #	Search Text	DBs	Time Stamp	Hits
30	BRS	L30	digital AND certificate AND client AND server AND authentication AND data AND transmission AND communication AND proof AND key AND updating AND validity AND control AND unit AND SSL AND TLS AND protocol AND mutual AND authentication AND order.CLM.	US-PGPUB	2007/09/20 19:02	3
31	BRS	L31	digital AND certificate AND client AND server AND authentication AND data AND transmission AND communication AND proof AND key AND updating AND validity AND control AND unit AND SSL AND TLS AND protocol AND mutual AND authentication AND order AND nodes.CLM.	US-PGPUB	2007/09/20 19:04	6
32	BRS	L32	digital AND certificate AND client AND server AND authentication AND data AND transmission AND communication AND proof AND key AND updating AND validity AND control AND unit AND SSL AND TLS AND protocol AND mutual AND authentication AND order AND nodes AND transmission AND destination.CLM.	US-PGPUB	2007/09/20 19:04	2

	Comments
30	
31	
32	

PORTAL
USPTO
Subscribe (Full Service) Register (Limited Service, Free) Login
Search: The ACM Digital Library The Guide
+root +key, +digital +certificate, +validation, +updating, +sh SEARCH
THE ACM DIGITAL LIBRARY
Feedback Report a problem Satisfaction survey

Terms used:
root key digital certificate validation updating shared private key mutual authentication certificate

Found 44 of 211,032

Sort results by relevance
Display results expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 44 Result page: 1 2 3 next

Relevance scale

1 Cryptography and data security
Dorothy Elizabeth Robling Denning
January 1982 Book
Publisher: Addison-Wesley Longman Publishing Co., Inc.
Full text available: pdf(19.47 MB) Additional Information: full citation, abstract, references, cited by, index terms

From the Preface (See Front Matter for full Preface)

Electronic computers have evolved from exiguous experimental enterprises in the 1940s to prolific practical data processing systems in the 1980s. As we have come to rely on these systems to process and store data, we have also come to wonder about their ability to protect valuable data.

Data security is the science and study of methods of protecting data in computer and communication systems from unauthorized disclosure ...

2 On interdomain routing security and pretty secure BGP (psBGP)
P.C. van Oorschot, Tao Wan, Evangelos Kranakis
July 2007 **ACM Transactions on Information and System Security (TISSEC)**, Volume 10 Issue 3
Publisher: ACM Press
Full text available: pdf(469.49 KB) Additional Information: full citation, abstract, references, index terms

It is well known that the Border Gateway Protocol (BGP), the IETF standard interdomain routing protocol, is vulnerable to a variety of attacks, and that a single misconfigured or malicious BGP speaker could result in large-scale service disruption. In this paper, we present *Pretty Secure BGP (psBGP)*---a proposal for securing BGP, including an architectural overview, design details for significant aspects, and preliminary security and operational analysis. psBGP differs from other secur ...

Keywords: BGP, authentication, certificates, interdomain routing, public-key infrastructure, secure routing protocols, trust

3 Fine-grained control of security capabilities
Dan Boneh, Xuhua Ding, Gene Tsudik
February 2004 **ACM Transactions on Internet Technology (TOIT)**, Volume 4 Issue 1

Publisher: ACM Press

Full text available: pdf(128.09 KB) Additional Information: full citation, abstract, references, citings, index terms

We present a new approach for fine-grained control over users' security privileges (fast revocation of credentials) centered around the concept of an on-line semi-trusted mediator (SEM). The use of a SEM in conjunction with a simple threshold variant of the RSA cryptosystem (mediated RSA) offers a number of practical advantages over current revocation techniques. The benefits include simplified validation of digital signatures, efficient certificate revocation for legacy systems and fast revocat ...

Keywords: Certificate Revocation, Digital Signatures, Public Key Infrastructure

4 Session M9: digital rights and marketing: Digital rights management using a mobile phone

Imad M. Abbadi, Chris J. Mitchell

August 2007 **Proceedings of the ninth international conference on Electronic commerce ICEC '07**

Publisher: ACM Press

Full text available: pdf(497.09 KB) Additional Information: full citation, abstract, references, index terms

This paper focuses on the problem of preventing illegal copying of digital assets without jeopardising the right of legitimate licence holders to transfer content between their own devices, which make up a domain. Our novel idea involves the use of a domain-specific mobile phone and the mobile phone network operator to authenticate the domain owner before devices can join a domain. This binds devices in a domain to a single owner, that, in turn, enables the binding of domain licences to the d ...

Keywords: 3GPP GAA, DRM, access control, authorised domain management, copyright protection, trusted computing

5 A public-key based secure mobile IP

John Zao, Joshua Gahm, Gregory Troxel, Matthew Condell, Pam Helinek, Nina Yuan, Isidro Castineyra, Stephen Kent

October 1999 **Wireless Networks**, Volume 5 Issue 5

Publisher: Kluwer Academic Publishers

Full text available: pdf(255.65 KB) Additional Information: full citation, references, citings, index terms

6 General storage protection techniques: Securing distributed storage: challenges, techniques, and systems

Vishal Kher, Yongdae Kim

November 2005 **Proceedings of the 2005 ACM workshop on Storage security and survivability StorageSS '05**

Publisher: ACM Press

Full text available: pdf(294.61 KB) Additional Information: full citation, abstract, references, index terms

The rapid increase of sensitive data and the growing number of government regulations that require longterm data retention and protection have forced enterprises to pay serious attention to storage security. In this paper, we discuss important security issues related to storage and present a comprehensive survey of the security services provided by the existing storage systems. We cover a broad range of the storage security literature, present a critical review of the existing solutions, compare ...

Keywords: authorization, confidentiality, integrity, intrusion detection, privacy

7 Access management for distributed systems: Peer-to-peer access control architecture using trusted computing technology
Ravi Sandhu, Xinwen Zhang
June 2005 **Proceedings of the tenth ACM symposium on Access control models and technologies SACMAT '05**
Publisher: ACM Press

Full text available: pdf(215.48 KB) Additional Information: full citation, abstract, references, citings, index terms, review

It has been recognized for some time that software alone does not provide an adequate foundation for building a high-assurance trusted platform. The emergence of industry-standard trusted computing technologies promises a revolution in this respect by providing roots of trust upon which secure applications can be developed. These technologies offer a particularly attractive platform for security in peer-to-peer environments. In this paper we propose a trusted computing architecture to enforce ac ...

Keywords: access control, policy enforcement, security architecture, trusted computing

8 Trustworthy 100-year digital objects: Evidence after every witness is dead
Henry M. Gladney
July 2004 **ACM Transactions on Information Systems (TOIS)**, Volume 22 Issue 3
Publisher: ACM Press

Full text available: pdf(1.24 MB) Additional Information: full citation, abstract, references, citings, index terms

In ancient times, wax seals impressed with signet rings were affixed to documents as evidence of their authenticity. A digital counterpart is a message authentication code fixed firmly to each important document. If a digital object is sealed together with its own audit trail, each user can examine this evidence to decide whether to trust the content---no matter how distant this user is in time, space, and social affiliation from the document's source.We propose an architecture and design that a ...

9 Secure sessions for Web services
Karthikeyan Bhargavan, Ricardo Corin, Cédric Fournet, Andrew D. Gordon
May 2007 **ACM Transactions on Information and System Security (TISSEC)**, Volume 10 Issue 2
Publisher: ACM Press

Full text available: pdf(579.98 KB) Additional Information: full citation, abstract, references, index terms

We address the problem of securing sequences of SOAP messages exchanged between web services and their clients. The WS-Security standard defines basic mechanisms to secure SOAP traffic, one message at a time. For typical web services, however, using WS-Security independently for each message is rather inefficient; moreover, it is often important to secure the integrity of a whole session, as well as each message. To these ends, recent specifications provide further SOAP-level mechanisms. WS-S ...

Keywords: Web services, XML security

10 Practical byzantine fault tolerance and proactive recovery
Miguel Castro, Barbara Liskov
November 2002 **ACM Transactions on Computer Systems (TOCS)**, Volume 20 Issue 4

Publisher: ACM Press

Full text available: pdf(1.63 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Our growing reliance on online services accessible on the Internet demands highly available systems that provide correct service without interruptions. Software bugs, operator mistakes, and malicious attacks are a major cause of service interruptions and they can cause arbitrary behavior, that is, Byzantine faults. This article describes a new replication algorithm, BFT, that can be used to build highly available systems that tolerate Byzantine faults. BFT can be used in practice to implement re ...

Keywords: Byzantine fault tolerance, asynchronous systems, proactive recovery, state machine replication, state transfer

11 A public-key based secure mobile IP

John Zao, Stephen Kent, Joshua Gahm, Gregory Troxel, Matthew Condell, Pam Helinek, Nina Yuan, Isidro Castineyra

September 1997 **Proceedings of the 3rd annual ACM/IEEE international conference on Mobile computing and networking MobiCom '97**

Publisher: ACM Press

Full text available: pdf(1.95 MB) Additional Information: full citation, references, citings

12 Strong password-only authenticated key exchange

David P. Jablon

October 1996 **ACM SIGCOMM Computer Communication Review**, Volume 26 Issue 5

Publisher: ACM Press

Full text available: pdf(1.52 MB) Additional Information: full citation, abstract, citings, index terms

A new simple password exponential key exchange method (SPEKE) is described. It belongs to an exclusive class of methods which provide authentication and key establishment over an insecure channel using only a small password, without risk of offline dictionary attack. SPEKE and the closely-related Diffie-Hellman Encrypted Key Exchange (DH-EKE) are examined in light of both known and new attacks, along with sufficient preventive constraints. Although SPEKE and DH-EKE are similar, the constraints a ...

13 Secure communications between bandwidth brokers

Bu-Sung Lee, Wing-Keong Woo, Chai-Kiat Yeo, Teck-Meng Lim, Bee-Hwa Lim, Yuxiong He, Jie Song

January 2004 **ACM SIGOPS Operating Systems Review**, Volume 38 Issue 1

Publisher: ACM Press

Full text available: pdf(922.33 KB) Additional Information: full citation, abstract, references

In the Differentiated Services (DiffServ) architecture, each domain has a Bandwidth Broker to provide the resources management, primarily bandwidth reservation. In a multi-domain environment, Simple Inter-domain Bandwidth Broker Signaling (SIBBS) protocol is proposed for the inter-domain communication protocol proposed for bandwidth broker communication. Since the information exchanged between BBs are sensitive in sense of Service Level Agreement (SLA), the communications between the inter-domai ...

Keywords: Bandwidth Broker, Public Key Infrastructure, Simple Inter-domain Bandwidth Broker Signaling

14 Computing curricula 2001

September 2001 **Journal on Educational Resources in Computing (JERIC)**
Publisher: ACM Press
Full text available: pdf(613.63 KB) html(2.78 KB) Additional Information: full citation, references, citings, index terms

15 Mobility support and location awareness: An approach to enhance inter-provider roaming through secret sharing and its application to WLANs
Ulrike Meyer, Jared Cordasco, Susanne Wetzel
September 2005 **Proceedings of the 3rd ACM international workshop on Wireless mobile applications and services on WLAN hotspots WMASH '05**
Publisher: ACM Press
Full text available: pdf(278.20 KB) Additional Information: full citation, abstract, references, index terms

In this paper, we show how secret sharing can be used to address a number of shortcomings in state-of-the-art public-key-based inter-provider roaming. In particular, the new concept does not require costly operations for certificate validation by the mobile device. It furthermore eliminates the need for a secure channel between providers upon roaming. We demonstrate the new approach by introducing a new protocol, EAP-TLS-KS, for roaming between 802.11i-protected WLANs. In addition, we show that ...

Keywords: 802.11i, EAP-TLS-KS, PKI, WLAN, distributed DSS, inter-provider roaming, micropayment scheme, secret sharing

16 Certificate-based authorization policy in a PKI environment
Mary R. Thompson, Abdelilah Essiari, Srilekha Mudumbai
November 2003 **ACM Transactions on Information and System Security (TISSEC)**, Volume 6 Issue 4
Publisher: ACM Press
Full text available: pdf(233.63 KB) Additional Information: full citation, abstract, references, citings, index terms

The major emphasis of public key infrastructure has been to provide a cryptographically secure means of authenticating identities. However, procedures for authorizing the holders of these identities to perform specific actions still need additional research and development. While there are a number of proposed standards for authorization structures and protocols such as KeyNote, SPKI, and SAML based on X.509 or other key-based identities, none have been widely adopted. As part of an effort to us ...

Keywords: Public key infrastructure, XML, digital certificates

17 Secure group management: Secure long term communities in ad hoc networks
Nicolas Prigent, Christophe Bidan, Jean-Pierre Andreaux, Olivier Heen
October 2003 **Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks SASN '03**
Publisher: ACM Press
Full text available: pdf(156.78 KB) Additional Information: full citation, abstract, references

Until recently, ad hoc networks were mainly used for military and security-sensitive applications. Nowadays, they could also be used in SOHO (Small Office / Home Office) or home networks. In such networks, devices are linked by long term relations. To ensure their security, it is necessary to define precisely which devices belong to a given network and are consequently inside the security perimeter. The chosen mechanisms need to be easy to use, because the users of SOHO and home networks are nei ...

Keywords: ad hoc networks security, home network security, secure long term community

18 Secure group management: Secure multicast groups on ad hoc networks

T. Kaya, G. Lin, G. Noubir, A. Yilmaz

October 2003 **Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks SASN '03**

Publisher: ACM Press

Full text available: pdf(212.24 KB) Additional Information: full citation, abstract, references, citings, index terms

In this paper we address the problem of secure multicast of data streams over a multihop wireless ad hoc network. We propose a dynamic multicast group management protocol that aims at solving problems that are specific to ad hoc networks such as mobility, unreliable links, and cost of multihop communication. The main idea is to have group members actively participate to the security of the multicast group, therefore reducing the communication and computation load on the source. Since the group s ...

Keywords: MANET, multihop ad hoc, secure multicast, tracking

19 Link and channel measurement: A simple mechanism for capturing and replaying wireless channels

Glenn Judd, Peter Steenkiste

August 2005 **Proceeding of the 2005 ACM SIGCOMM workshop on Experimental approaches to wireless network design and analysis E-WIND '05**

Publisher: ACM Press

Full text available: pdf(6.06 MB) Additional Information: full citation, abstract, references, index terms

Physical layer wireless network emulation has the potential to be a powerful experimental tool. An important challenge in physical emulation, and traditional simulation, is to accurately model the wireless channel. In this paper we examine the possibility of using on-card signal strength measurements to capture wireless channel traces. A key advantage of this approach is the simplicity and ubiquity with which these measurements can be obtained since virtually all wireless devices provide the req ...

Keywords: channel capture, emulation, wireless

20 T1-B: computer and network security symposium: Multiple personal security domains

Reinaldo Matushima, Yeda R. Venturini, Rony R. M. Sakuragui, Tereza C. M. B. Carvalho, Wilson V. Ruggiero, Mats Naslund, Makan Pourzandi

July 2006 **Proceedings of the 2006 international conference on Wireless communications and mobile computing IWCMC '06**

Publisher: ACM Press

Full text available: pdf(503.77 KB) Additional Information: full citation, abstract, references, index terms

Mobility, usability and security are major requirements for any Ad Hoc network systems, and there have been numerous papers in regards to them. However, often these requirements are addressed separately. For a valid solution, these requirements must be considered from an integrated view. In this paper, taking into account mobility and usability, we implement a framework which allows to securely share resources and services between devices in Ad-hoc networks, based on security policies defined by ...

Keywords: ad hoc, domains composition, personal networks, security domains, security enforcement layer, wireless networks

Results 1 - 20 of 44 Result page: **1** 2 3 next

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2007 ACM, Inc.
Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player

Web Images Video News Maps Gmail more ▾ Sign in

Google proof key, update, validation, shared private ke Search Advanced Search Preferences
New! View and manage your web history

Web Results **1 - 10** of about **24,300** for **proof key, update, validation, shared private key, mutual authenticat**

nsslabs.com | Public **Key** Infrastructure | **Key**, **Certificate**, Pki ...
Automatic **key update** – The only reason for a **certificate** to have an expiry ..... its own **private** Root Signing **Key** - thus creating a **digital certificate** for ...
nsslabs.com/content/view/18/102/ - 111k - Cached - Similar pages

Cryptography - **Key** Management patents
A **key validation** service (KVS) provides the ability to assess the validity ... the user first sends **proof** to the KVS that the user's **private key** is valid. ...
www.freshpatents.com/x1380277000psbc.php - 76k - Cached - Similar pages

CommsDesign - Public **Key** Infrastructure Overview
Automatic **Key Update**—The only reason for a **certificate** to have an expiry date is to .... only public keys, and no **private key** is ever transmitted or **shared**. ...
www.commsdesign.com/showArticle.jhtml?articleID=192200379 - 75k - Cached - Similar pages

[PDF] X.509 **Certificate** Policy for the Common Policy Framework ...
File Format: PDF/Adobe Acrobat - View as HTML
authentication servers), they are considered a single subscriber and may **share** the **private key**. corresponding to a **certificate** issued under this policy.] ...
www.cio.gov/fpkipa/documents/EGovCA-CP.pdf - Similar pages

[PDF] X.509 **Certificate** Policy For The Federal Bridge Certification ...
File Format: PDF/Adobe Acrobat - View as HTML
digital certificate by the Entity. The trusted person will present information ..... The list of those holding the **shared private key** must be provided to, ...
www.cio.gov/fpkipa/documents/fbca_cp_09-10-02.pdf - Similar pages
[More results from www.cio.gov]

[PDF] Microsoft PowerPoint - 03_Grid_security
File Format: PDF/Adobe Acrobat - View as HTML
X.509 **Digital certificate** is the basis of **Authentication** in major ... **Private key** is used to sign a proxy **certificate** with its own, new. public/**private key** ...
gridcourse.fe.up.pt/slides/1_3.pdf - Similar pages

[PDF] 3GPP TR 33.919
File Format: PDF/Adobe Acrobat - View as HTML
A number of applications **share** a need for **mutual authentication** between a ..... The (public, **private**) **key** pair and the corresponding **digital certificate** can ...
www.arib.or.jp/IMT-2000/V620May07/3_T12/ARIB-TR-T12/Rel7/33/A33919-720.pdf - Similar pages

Digital certificate management system, **digital certificate** ...
A **digital certificate** management apparatus updates a **proof key** used for proving ... to safely **update** an **authentication** public **key** used for **validation** of a ...
www.freepatentsonline.com/20040243805.html - 330k - Cached - Similar pages

Java Security Packages JCA/JCE (an outline) In this tutorial, the ...
A **certificate** becomes invalid after the expiry of **validation** period. Sometimes, the **private key** associated with a public **key** gets compromised (ie) exposed, ...

www.roseindia.net/java/java-security.shtml - 32k - Cached - Similar pages

[PDF] UNITED STATES DEPARTMENT OF AGRICULTURE NATIONAL FINANCE CENTER ...
File Format: PDF/Adobe Acrobat - View as HTML
authenticated using that **certificate's** associated **private key**, ... **Mutual Authentication**.
Occurs when parties at both ends of a communication activity ...
sig.nfc.usda.gov/pki/nfccp/cp-5-27-05.pdf - Similar pages

1 2 3 4 5 6 7 8 9 10 **Next**

Try Google Desktop: search your computer as easily as you search the web.

proof key, update, validation, shared Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

©2007 Google - Google Home - Advertising Programs - Business Solutions - About Google

IEEE Xplore® RELEASE 2.4

Home | Login | Logout | Access Information | Alerts | Purchase History | Cart |

Welcome United States Patent and Trademark Office

Search Results BROWSE SEARCH IEEE XPLORE GUIDE

Results for "(proof key, validation, updating, shared private key, mutual authentication, certificate<in>..." e-mail
Your search matched **176098** of **1643271** documents.
A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

» Search Options

View Session History

New Search

» Other Resources
(Available For Purchase)

Top Book Results

Automated Defect Prevention
by Kolawa, A.;Huizinga, D.;
Hardcover, Edition: 1

Guidance for the Verification and Validation of Neural Networks
by Darrah, M. A.;Taylor, B. J.;Pullum, L. L.;
Paperback, Edition: 1

Semiconductor Material and Device Characterization
by Schroder, D. K.;
Hardcover, Edition: 1

Electromagnetic Fields
by Bladel, J. G. V.;
Hardcover, Edition: 1

Fundamentals of Telecommunications
by Freeman, R. L.;
Hardcover, Edition: 1

View All 50 Result(s)

» Key

IEEE JNL	IEEE Journal or Magazine
IET JNL	IET Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IET CNF	IET Conference Proceeding
IEEE STD	IEEE Standard

Modify Search

(proof key, validation, updating, shared private key, mutual authentication, certificate Search

Check to search only within this results set

Display Format: Citation Citation & Abstract

view selected items Select All Deselect All View: 1-25 | 26-5

1. **DICTATE: DIstributed CerTification Authority with probabilisTic frEshnes networks**
Jun Luo; Hubaux, J.-P.; Eugster, P.T.;
Dependable and Secure Computing, IEEE Transactions on
Volume 2, Issue 4, Oct.-Dec. 2005 Page(s):311 - 323
Digital Object Identifier 10.1109/TDSC.2005.49
AbstractPlus | Full Text: PDF(640 KB) IEEE JNL
Rights and Permissions

2. **Security and trust issues in ubiquitous environments - the business-to-e dimension**
Walter, T.; Bussard L; Robinson, P.; Roudier, Y.;
Applications and the Internet Workshops, 2004. SAINT 2004 Workshops. 2004 Symposium on
26-30 Jan. 2004 Page(s):696 - 701
Digital Object Identifier 10.1109/SAINTW.2004.1268723
AbstractPlus | Full Text: PDF(294 KB) IEEE CNF
Rights and Permissions

3. **A survey of PKI components and scalability issues**
Slagell, A.; Bonilla, R.; Yurcik, W.;
Performance, Computing, and Communications Conference, 2006. IPCCC 20(International
10-12 April 2006 Page(s):10 pp.
Digital Object Identifier 10.1109/.2006.1629442
AbstractPlus | Full Text: PDF(192 KB) IEEE CNF
Rights and Permissions

4. **Certificate revocation and certificate update**
Naor, M.; Nissim, K.;
Selected Areas in Communications, IEEE Journal on
Volume 18, Issue 4, April 2000 Page(s):561 - 570
Digital Object Identifier 10.1109/49.839932
AbstractPlus | References | Full Text: PDF(156 KB) IEEE JNL
Rights and Permissions

5. **A new on-line certificate validation method using LDAP component matc**
Jong Hyuk Choi; Sang Seok Lim; Zeilenga, K.D.;

Systems, Man and Cybernetics (SMC) Information Assurance Workshop, 2005 from the Sixth Annual IEEE
15-17 June 2005 Page(s):280 - 285
Digital Object Identifier 10.1109/IAW.2005.1495964
AbstractPlus | Full Text: PDF(361 KB) IEEE CNF
Rights and Permissions

6. **Certificate management in ad hoc networks**
Morogan, M.C.; Muftic, S.;
Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposiur
27-31 Jan. 2003 Page(s):337 - 341
AbstractPlus | Full Text: PDF(354 KB) IEEE CNF
Rights and Permissions

7. **Simplifying PKI usage through a client-server architecture and dynamic p certificate paths and repository addresses**
Hunter, B.;
Database and Expert Systems Applications, 2002. Proceedings. 13th Internati
2-6 Sept. 2002 Page(s):505 - 510
AbstractPlus | Full Text: PDF(264 KB) IEEE CNF
Rights and Permissions

8. **A flexible scheme for on-line public-key certificate status updating and v**
Faldella, E.; Prandini, M.;
Computers and Communications, 2002. Proceedings. ISCC 2002. Seventh Int Symposium on
1-4 July 2002 Page(s):891 - 898
Digital Object Identifier 10.1109/ISCC.2002.1021778
AbstractPlus | Full Text: PDF(461 KB) IEEE CNF
Rights and Permissions

9. **IEEE Standard for Information technology- Telecommunications and info exchange between systems- Local and metropolitan area networks- Spec requirements Part 11: Wireless LAN Medium Access Control (MAC) and F (PHY) specifications Amendment 6: Medium Access Control (MAC) Secu Enhancements**
2004 Page(s):0_1 - 175
AbstractPlus | Full Text: PDF(2342 KB) IEEE STD

10. **IEEE Standard for Local and metropolitan area networks Part 16: Air Inte and Mobile Broadband Wireless Access Systems Amendment 2: Physica Access Control Layers for Combined Fixed and Mobile Operation in Lice Corrigendum 1**
2006 Page(s):0_1 - 822
AbstractPlus | Full Text: PDF(5468 KB) IEEE STD

11. **Performance analysis of scalable certificate revocation schemes for ad h**
Eichler, S.; Muller-Rathgeber, B.;
Local Computer Networks, 2005. 30th Anniversary. The IEEE Conference on
15-17 Nov. 2005 Page(s):9 pp.
Digital Object Identifier 10.1109/LCN.2005.105
AbstractPlus | Full Text: PDF(288 KB) IEEE CNF
Rights and Permissions

12. **A performance study of over-issuing delta-CRLs with distribution points**
Rojanapasakorn, A.; Sathitwiriyawong, C.;
Advanced Information Networking and Applications, 2004. AINA 2004. 18th In Conference on
Volume 2, 2004 Page(s):178 - 181 Vol.2

Digital Object Identifier 10.1109/AINA.2004.1283781

AbstractPlus | Full Text: PDF(253 KB) IEEE CNF
Rights and Permissions

13. **Caching alternatives for a MANET-oriented OCSP scheme**
Marias, G.F.; Papapanagiotou, K.; Georgiadis, P.;
Security and Privacy for Emerging Areas in Communication Networks, 2005. V
1st International Conference on
5-9 Sept. 2005 Page(s):209 - 217
Digital Object Identifier 10.1109/SECCMW.2005.1588315

AbstractPlus | Full Text: PDF(156 KB) IEEE CNF
Rights and Permissions

14. **FlexiCert: merging X.509 identity certificates and attribute certificates**
Lakshminarayanan, A.; Jianying Zhou;
Database and Expert Systems Applications, 2003. Proceedings. 14th Internati
1-5 Sept. 2003 Page(s):489 - 493
Digital Object Identifier 10.1109/DEXA.2003.1232071

AbstractPlus | Full Text: PDF(229 KB) IEEE CNF
Rights and Permissions

15. **Security aspects in standard certificate revocation mechanisms: a case s**
Berbecaru, D.; Lioy, A.; Marian, M.;
Computers and Communications, 2002. Proceedings. ISCC 2002. Seventh Int
Symposium on
1-4 July 2002 Page(s):484 - 489
Digital Object Identifier 10.1109/ISCC.2002.1021719

AbstractPlus | Full Text: PDF(257 KB) IEEE CNF
Rights and Permissions

16. **Using virtual organizations membership system with EDG's grid security access**
Niinimaki, M.; White, J.; de Cerff, W.S.; Hahkala, J.; Niemi, T.; Pitkanen, M.;
Database and Expert Systems Applications, 2004. Proceedings. 15th Internati
30 Aug.-3 Sept. 2004 Page(s):517 - 522
Digital Object Identifier 10.1109/DEXA.2004.1333527

AbstractPlus | Full Text: PDF(355 KB) IEEE CNF
Rights and Permissions

17. **Active certificates: a new paradigm in digital certificate management**
Mukkamala, R.; Balusani, S.;
Parallel Processing Workshops, 2002. Proceedings. International Conference
18-21 Aug. 2002 Page(s):30 - 37
Digital Object Identifier 10.1109/ICPPW.2002.1039709

AbstractPlus | Full Text: PDF(398 KB) IEEE CNF
Rights and Permissions

18. **Information technology- Telecommunications and information exchange systems- Local and metropolitan area networks- Specific requirements- I LAN Medium Access Control (MAC) and Physical Layer (PHY) Specificati**
2003 Page(s):i - 513

AbstractPlus | Full Text: PDF(6325 KB) IEEE STD

19. **Evaluation of certificate revocation policies: OCSP vs. Overissued-CRL**
Munoz, J.L.; Forne, J.; Castro, J.C.;
Database and Expert Systems Applications, 2002. Proceedings. 13th Internati
2-6 Sept. 2002 Page(s):511 - 515

AbstractPlus | Full Text: PDF(741 KB) IEEE CNF

Rights and Permissions

20. **Self-managed heterogeneous certification in mobile ad hoc networks**
Weihong Wang; Ying Zhu; Baochun Li;
Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th
Volume 3, 6-9 Oct. 2003 Page(s):2137 - 2141 Vol.3
Digital Object Identifier 10.1109/VETECF.2003.1285402
AbstractPlus | Full Text: PDF(251 KB) IEEE CNF
Rights and Permissions

21. **A Study on Establishment of Secure RFID Network Using DNS Security E**
YoungHwan Ham; NaeSoo Kim; CheolSig Pyo; JinWook Chung;
Communications, 2005 Asia-Pacific Conference on
03-05 Oct. 2005 Page(s):525 - 529
AbstractPlus | Full Text: PDF(336 KB) IEEE CNF
Rights and Permissions

22. **IEEE Std 802.11-1997 Information Technology- telecommunications And exchange Between Systems-Local And Metropolitan Area Networks-spec Requirements-part 11: Wireless Lan Medium Access Control (MAC) And I (PHY) Specifications**
18 November 1997 Page(s):i - 445
AbstractPlus | Full Text: PDF(25764 KB) IEEE STD

23. **A simulation study of over-issuing delta-CRLs with distribution points**
Rojanapasakorn, A.; Sathitwiriyawong, C.;
TENCON 2004. 2004 IEEE Region 10 Conference
Volume B, 21-24 Nov. 2004 Page(s):21 - 24 Vol. 2
Digital Object Identifier 10.1109/TENCON.2004.1414521
AbstractPlus | Full Text: PDF(1860 KB) IEEE CNF
Rights and Permissions

24. **On certificate-based security protocols for wireless mobile communicati**
Chang-Seop Park;
Network, IEEE
Volume 11, Issue 5, Sept.-Oct. 1997 Page(s):50 - 55
Digital Object Identifier 10.1109/65.620522
AbstractPlus | Full Text: PDF(1492 KB) IEEE JNL
Rights and Permissions

25. **Restricting access with certificate attributes in multiple root environment certificate masquerading**
Hayes, J.M.;
Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings
10-14 Dec. 2001 Page(s):386 - 390
AbstractPlus | Full Text: PDF(167 KB) IEEE CNF
Rights and Permissions

View: **1-25** | 26-5

Indexed by Inspec®

© Copyright 2006 IEEE –